SPAWAR
Systems Center
PACIFIC

TECHNICAL REPORT 3055
September 2016

Radio Signal Augmentation for Improved Training of a Convolutional Neural Network

Daniel Gebhardt, Ph.D.
Benjamin Migliori, Ph.D.
Logan Straatemeier
Michael Walton

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

K. J. Rothenhaus, CAPT, USN
Commanding Officer

C. A. Keeney
Executive Director

ADMINISTRATIVE INFORMATION

The work described in this report was performed by the IO Support to National Security Branch (Code 56120), the IO Spectrum Exploitation Branch (Code 56140), and Exploitation Systems Branch (Code 56150) of the Information Operations Division (Code 56100), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA. The Naval Innovative Science and Engineering (NISE) Program at SSC Pacific funded this Applied Research project.

Released by
E. R. Buckland, Head
IO Support to National Security Branch

Under authority of
G. Settelmayer, Head
Information Operations Division

SB

EXECUTIVE SUMMARY

This technical report presents the findings of an experiment to evaluate the effectiveness of our technique for improving the accuracy of identifying which type of digital modulation is present in a sample of radio signal data. We use a convolutional neural network (CNN) to identify the modulation type from raw digitized radio signal input. The CNN is trained using our technique of dataset augmentation, which applies a transformation specific to the sensory domain of radio (and potentially, closely related signal types). This augmentation simulates a receiver's clock offset or error.

Digital radio signal receivers will have a clock frequency slightly different than the transmitter, even if each is tuned to the "same" frequency. This is usually accounted for in the receiver design, referred to as carrier clock recovery, since it is designed for a known signal type. Our method is to apply varying amounts of clock frequency offset to a training dataset, and use it to train the machine learning algorithm (in this case, a CNN). The trained CNN model is compared to a baseline model in which no clock offset was used during training.

Classification performance increases to nearly 100% when trained with frequency offset compared to the baseline of 58%. Two real-world signals were captured from car remote keyless entry fobs. These signals contain an unknown receiver clock offset. The network trained with a our method classified nearly 100% of the samples correctly, while the baseline network did not correctly identify the on-off keying (OOK) modulation.

A recommended action is to further investigate dataset augmentation, especially in the domain of radio signals. This domain could benefit from very specific, but very useful, transforms to further improve performance of machine learning techniques.

This work was done as part of the BIAS (Biologically Inspired Autonomous Sensing) project, funded by the Naval Innovative Science and Engineering (NISE) Program.

CONTENTS

Figures

Tables

1. INTRODUCTION

Artificial neural networks, and specifically deep convolutional neural networks (CNNs), are a top-performing technology to detect and classify features of interest in sensory input data. The most common input data is imagery, audio, and text data, with the output providing a descriptive label of an image [1] or music [2], for example. Defense Advanced Research Project Agency (DARPA) and other Department of Defense (DoD) agencies have funded research in this field, and private industry has also heavily invested. Generally, CNNs and related machine learning approaches are a quickly growing and potentially disruptive technology in many application areas.

A growing domain for the application of machine learning techniques is in signal processing, specifically radio signals. Automatic modulation classification (AMC) is the task of identifying the type (or class) of modulation applied to a received radio signal. Many methods have been proposed for this task [3], with recent attempts using neural network approaches [4, 5].

A common problem for radio signal receivers is a clock frequency mismatch, error, or difference, between it and the transmitter that produced the signal [6]. The motivation for this work is that this clock frequency mismatch negatively aects classification accuracy of the techniques presented in [4]. The example in Figure 1 shows how the in-phase/quadrature (I/Q) samples composing a symbol of data modulated by phase-shift keying (PSK), "drift" when a receiver's clock is not matched.

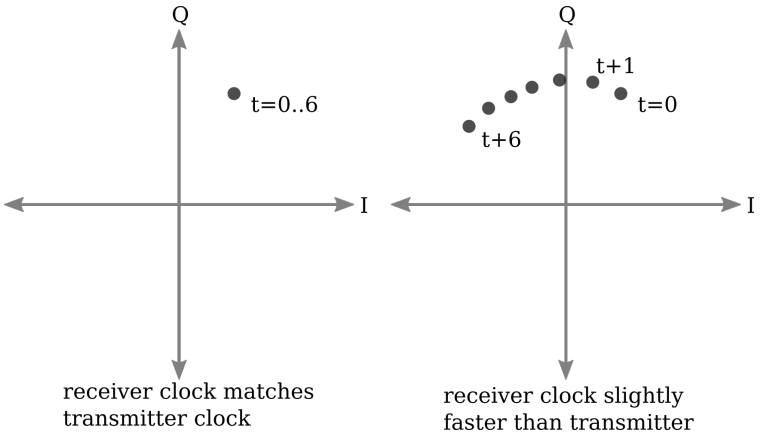


Figure 1. Effect of receiver frequency error on samples representing a PSK modulation symbol.

This difference can be estimated and corrected for in a process called *carrier recovery*. While many carrier recovery methods exist, it is a more challenging task with no knowledge of the signal's modulation type, or even the expected center frequency. Carrier recovery may also introduce latency in processing a radio signal—latency that may not be acceptable for certain applications, especially if the goal is not to completely demodulate the signal into a bitstream.

Our machine learning method attempts to incorporate receiver clock mismatch into the training process itself, rather than performing carrier recovery in a separate processing step.

2. METHODS AND EXPERIMENT

2.1 CNN CONFIGURATION

A CNN configuration defines the architecture and architectural parameters of the network. Examples of these parameters include:

- Input data dimensions and channels (e.g., image size and colors)
- Size of convolutional filters
- Number of convolutional filters
- Pooling/downsampling size and method (e.g., max-pool or average)
- Number of convolution and pooling layers
- Size and number of fully connected (dense) layers
- Output representation size and type (e.g., the number of classes of the input dataset and the predicted class of an input sample)

In this experiment, the data and CNN configuration was specified as follows, and also shown in Figure 2:

- Input is two channels (for the I and Q portion of the RF sample) of length 225
- Convolution Layer 1: 64 filters of 5-wide windows, for each of the two channels
- Maxpool Layer 1: a 3-wide window
- Convolution Layer 2: 64 filters of 3-wide windows
- Maxpool Layer 2: a 3-wide window
- Fully Connected Layer 1: 100 neurons
- Fully Connected Layer 2 (output): six neurons, one for each class, trained with softmax loss function

2.2 DATASETS

The datasets were formed from two sources: synthetically generated data and "live capture" radio signals from actual devices.

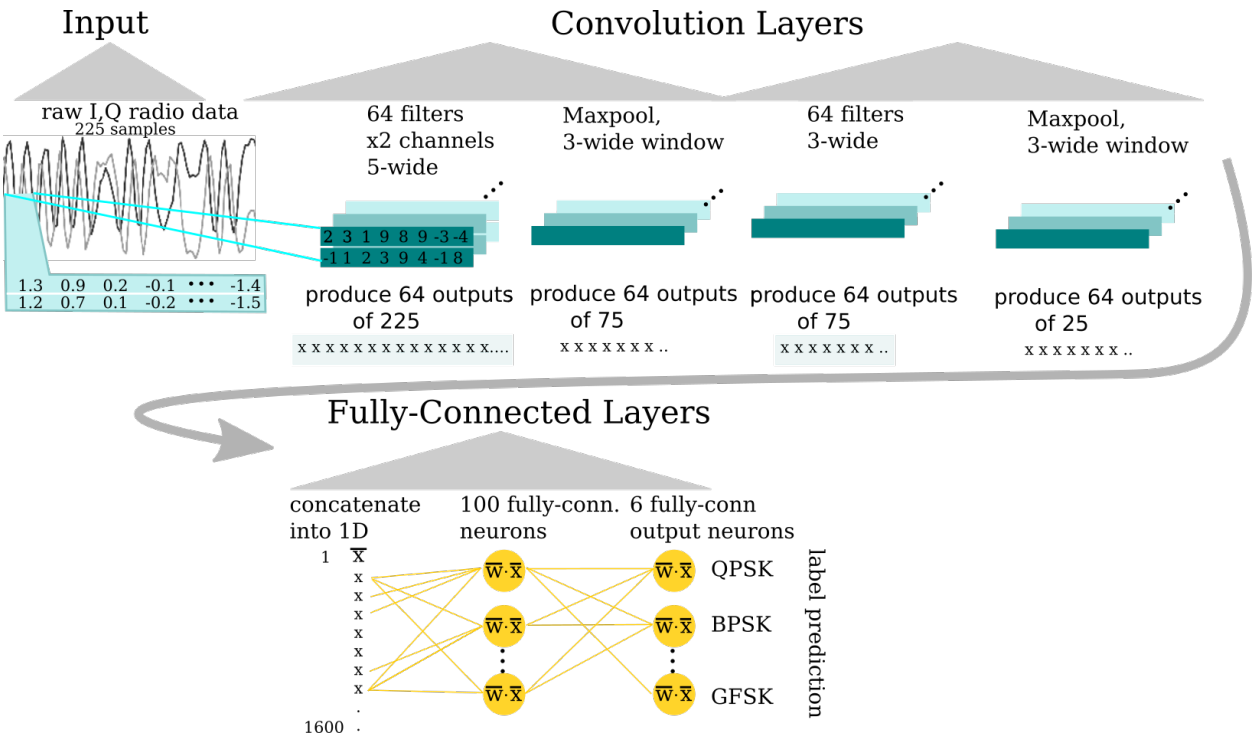


Figure 2. Basic CNN architecture for radio modulation classification.

2.2.1 Synthetic Signals

The synthetically generated radio signals clean of outside interference. We used the GNU Radio [7] software-defined radio (SDR) framework to construct the modulations that generated this data.

A binary file, produced by randomly choosing byte values $[0, 255]$, is the waveforms' input. This binary data is modulated as I/Q samples using each of six methods: on-off keying (OOK), Gaussian frequency-shift keying (GFSK), Gaussian minimum-shift keying (GMSK), dierential binary phase-shift keying (DBPSK), dierential quadrature phase-shift keying (DQPSK), and orthogonal frequency-division multiplexing (OFDM).

For each modulation, the samples are sent to a Nuand™ BladeRF™ software-defined radio (SDR), where they are upconverted to the carrier frequency. The SDR is configured in RF loop-back mode, such that the RF signal is sent and received only within the device's circuitry, and not to an external antenna. This arrangement provides added realism by incorporating the upconversion and radio effects, but without unwanted third-party signals that could pollute the controlled testing.

The signal sampling rate is set so that the number of samples per symbol (N_{SpS}) is consistent for every modulation type, except for OFDM. In contrast with the other modulation techniques, OFDM encodes data on multiple carrier frequencies simultaneously, within the same symbol, and modulates each carrier frequency independently. Our experiment used an existing OFDM signal processing component that operates with a symbol rate different than the other configurations, but with the same sample rate. This rate is identical for both the

transmission and reception of the signal. The received RF signal is down-converted at the radio and the resulting I/Q samples are stored for analysis.

The data files need to be arranged into a format and structure for use by our neural network. The I/Q data are split into segments consisting of N_{SpV} samples, or samples per vector. A segment is composed of interleaved I and Q values for each sample, forming a vector of length $2 \times N_{SpV}$. Thus, each vector contains $\frac{N_{SpV}}{N_{SpS}}$ symbols. These vectors are placed into two sets, *train* and *test* (sizes N_{Vtrain} and N_{Vtest}), such that both the modulation type and positions within the set are random. The parameter N_{SpV} is identical for each modulation type for all experiments described in this paper. The specific values of all parameters are shown in Table 1. Example vectors of this dataset is plotted in Figure 3. Notice how the I and Q values drift over the course of the input vector. This is especially obvious in the OOK modulation. Another observation is that GFSK appers very similar to the unaltered baseline dataset. This is to be expected, because FSK does not rely on a fixed sample point in I/Q space (opposed to QPSK, where the location determines the symbol). Thus, one might hypothesize the FSK classification would be easy to detect even if the receiver has a frequency mismatch.

Table 1. Data generation parameters.

Description	Parameter	Value
Samples per symbol	N_{SpS}	10
Samples per vector	N_{SpV}	225
Number of training vectors	N_{Vtrain}	60000
Number of training vectors per modulation	N_{Vmod}	10000
Number of test vectors	N_{Vtest}	10000

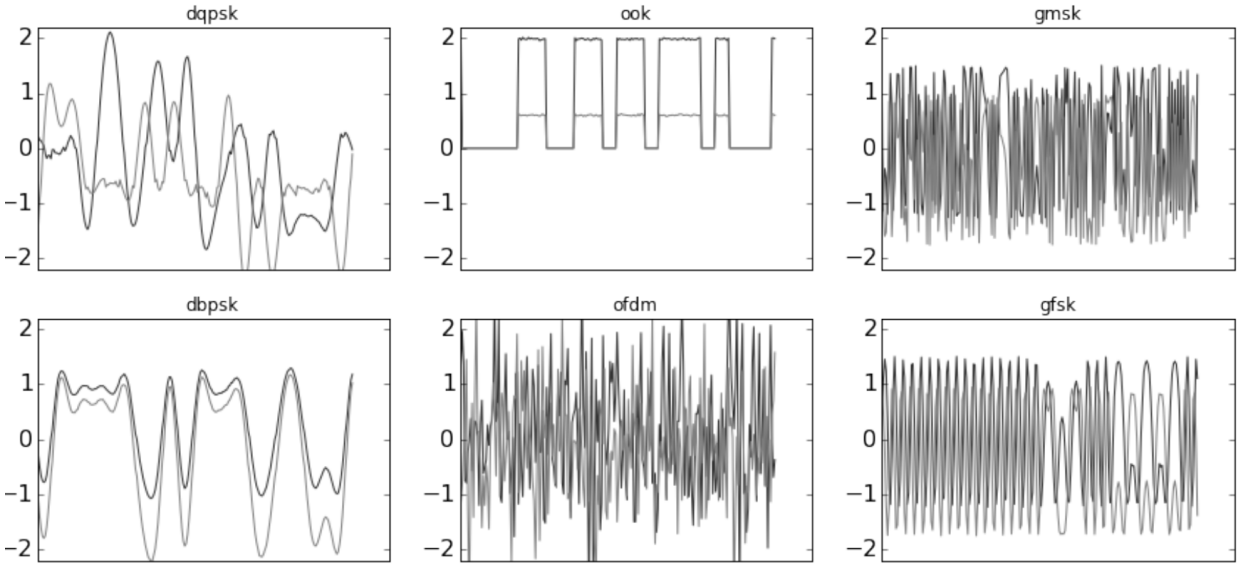


Figure 3. Sample I and Q vectors from the synthetic dataset.

2.2.2 Application of Frequency Offset

Another dataset was generated from the baseline dataset described above, in which the I and Q samples are adjusted to simulate a receiver's frequency mismatch. The algorithm to apply this offset is described as follows: for each input vector (a "clip" of 225 samples), choose an offset fraction, δ_f, within range $[-0.02, +0.02]$, where δ is chosen with a uniform random distribution with the range. For example, if 0.01 was chosen for a vector, each sample (I, Q point) in the vector is rotated sequentially by $2\pi \times 0.01$ radians. These range values were simply chosen experimentally, and to simulate a mild clock error. The altered dataset samples are shown in Figure 4.

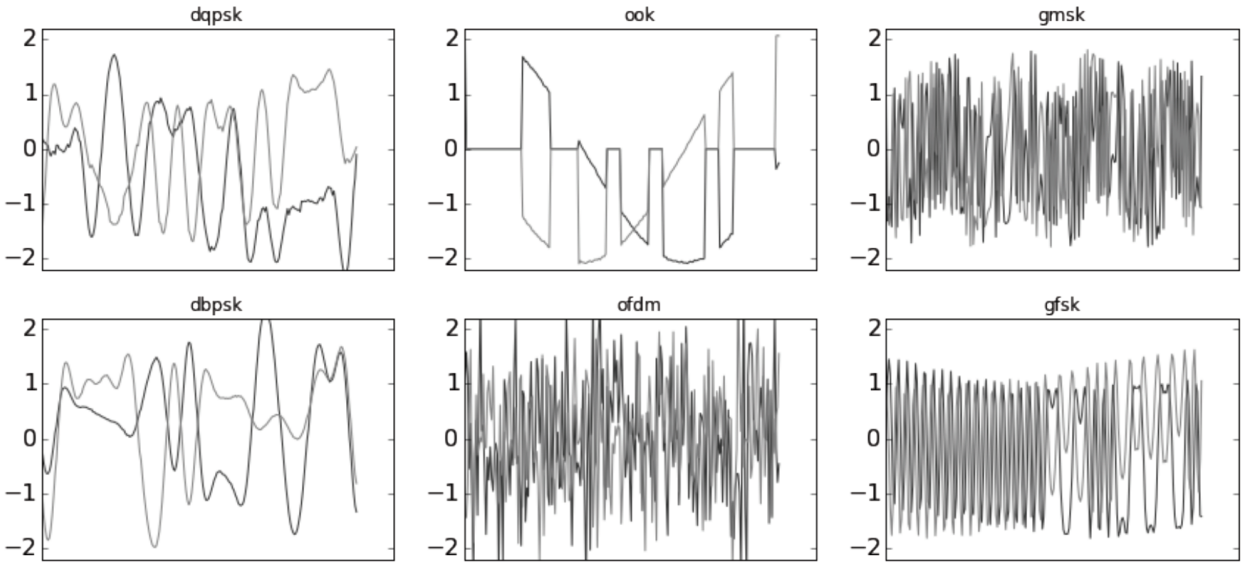


Figure 4. Sample I and Q vectors altered with a frequency offset.

2.2.3 Real Device Signals

Two real-world signals were captured from vehicle remote keyless entry (RKE) fobs: one was FSK modulated and the other was OOK modulated, which were determined with manual inspection of the signals. We can use this data to validate how well our AMC does on a completely new input source, one that it hasn't been trained against. Validation is important to see if the neural network overfit during training, or learned some "bad" features of the data that do not truly represent the difference in modulation. For example, it may learn that "it must be OOK if there is a sample point above value 2.0," which is not a feature that truly separates OOK from other modulations. The receiver was tuned to 315 MHz, which was approximately the experimentally verified center frequency of the two transmitters. The sample rate of the SDR was 100 KHz. These real signals replace the data in the GFSK and OOK synthetic dataset, and examples are shown in Figure 5.

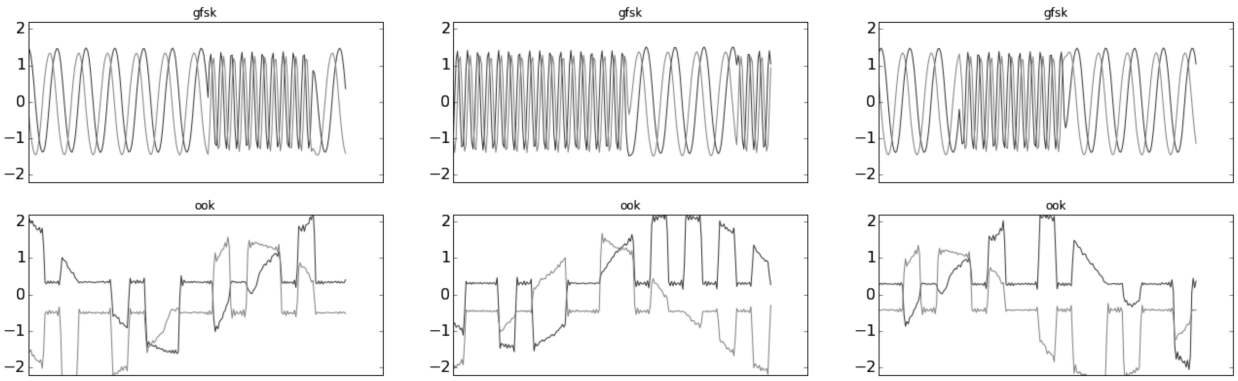


Figure 5. Sample I and Q vectors from remote keyless entry fobs.

2.3 EXPERIMENT CONFIGURATION

Two CNN models are created with the architecture described in Section 2.1. One model, $\mathcal{M}_{clean}$, was trained on the clean synthetic dataset with no clock offset applied. The other model, $\mathcal{M}_{offset}$, was trained on the synthetic dataset that had the clock offsets applied.

2.3.1 Synthetic Data Experiment

Each model is tested (evaluated) on the synthetic dataset that contains a clock offset. We use the *test* subset of the dataset that had not been used during training to avoid data snooping and overfitting, both of which can cause an optimistic classification performance.

2.3.2 Additional Frequency Offset Experiment

This experiment used the synthetic test dataset that has been altered in the following way to evaluate each model. First, the GFSK synthetic data has been replaced with the real device data from the FSK-modulated RKE. Second, a greater amount of frequency offset was applied, with $\delta_f = [-0.05, +0.05]$. This offset was applied to the real data as well.

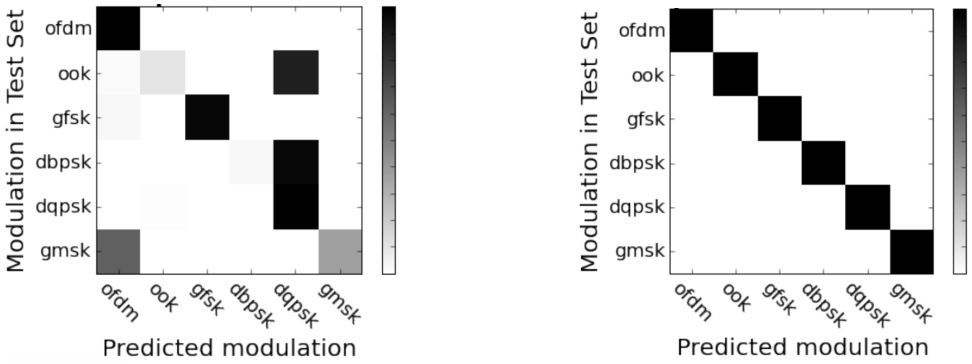
2.3.3 Real Signal Data Experiment

The final experiment evaluated both $\mathcal{M}_{clean}$ and $\mathcal{M}_{offset}$ on only real data captured from the remote keyless entries (RKEs). The models still decide to which of the six modulations the unknown input belongs, but there are only two actual modulation types in the dataset (FSK and OOK).

3. RESULTS AND DISCUSSION

3.1 SYNTHETIC DATA

The Synthetic Data Experiment results are shown in Figure 6 in the form of a *confusion matrix*. A confusion matrix plots the percent of correct classifications as a grayscale (darker is higher percentage) for each combination of true labels and predicted labels. True labels are shown in the Y-axis and predicted labels on the X-axis, and this plot can be quickly interpreted with correct classifications appearing on the matrix diagonal.



(a) Without clock offset augmentation

(b) With clock offset augmentation

Figure 6. Confusion matrices comparing of models trained without ($\mathcal{M}_{clean}$) and with ($\mathcal{M}_{offset}$) clock offset in the synthetic dataset.

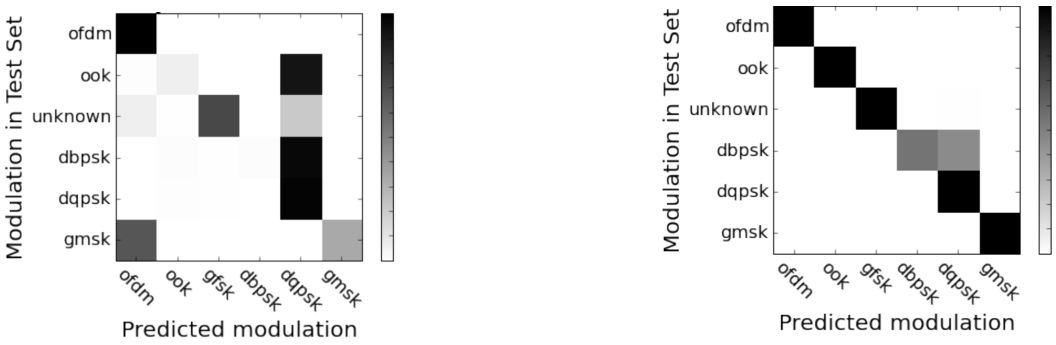
Classification accuracy improved dramatically when the model was trained with the frequency offset augmented dataset, raising from 58% overall accuracy for $\mathcal{M}_{clean}$ to 100% for $\mathcal{M}_{offset}$. Note how the FSK modulation type is not affected by the frequency augmentation, and is correctly identified in the network trained with no augmentation. This is due to the nature of the modulation, which does not rely on fixed I/Q constellation points, but on relative changes in frequency between symbols.

3.2 ADDITIONAL FREQUENCY OFFSET

The Additional Frequency Offset Experiment results are shown in Figure 7. It appears that the addition of even greater frequency ofset did not generally worsen classification performance compared to the lesser offset used during training, which indicates the $\mathcal{M}_{offset}$ model learned features in the signal that generalize well to new, but related, signals. The notable exception is the additional confusion between BPSK and QPSK (binary and quad phase-shift keying). This observation intuitively makes sense, considering their similarity, as both fall under the family of M-ary phase shift modulations. The real signal from a RKE fob was identified correctly in the majority of cases. There were 11 inputs misclassified and 1615 correctly classified as FSK.

3.3 REAL SIGNAL DATA

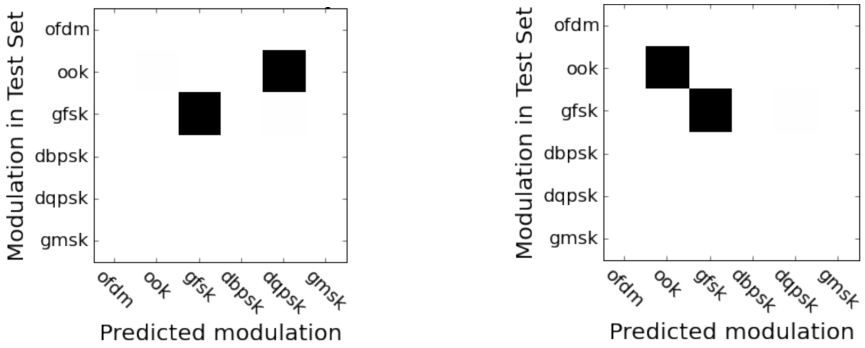
The RKE signal capture dataset test results are shown in Figure 8, which compares models $\mathcal{M}_{clean}$ and $\mathcal{M}_{offset}$. Both models could correctly identify the FSK signal for most samples,



(a) $\mathcal{M}_{clean}$ (b) $\mathcal{M}_{offset}$

Figure 7. Comparison between models where clock offset δ_f has been increased to: $[-0.05, +0.05]$. Label "unknown" is a real signal modulated as FSK.

with 99.4% accuracy. However the OOK signal was not correctly identified by $\mathcal{M}_{clean}$ (27 correct and 4614 incorrect OOK samples). Classification accuracy improved greatly in $\mathcal{M}_{offset}$, with all 4641 OOK samples were correctly classified.



(a) $\mathcal{M}_{clean}$ (b) $\mathcal{M}_{offset}$

Figure 8. Confusion matrices comparing of models trained without ($\mathcal{M}_{clean}$) and with ($\mathcal{M}_{offset}$) clock offset, and tested on the real RF signals.

3.4 UNSANITIZED REAL-TIME SIGNAL CLASSIFICATION

The results in this section are qualitative in their description, and included as supplementary material to aid in future work and analysis. We performed informal experiments to identify the modulation types of unknown and "unsanitized" signals in real-time. That is to say, the signals were not captured, stored, converted into a dataset, and replayed in a controlled manner as in Section 3.3. The real-time characteristic is due to the experimental system capturing RF signals and providing a modulation classification as soon as the computation is complete. The benefit to this setup is the user can quickly experiment with various transmitters to glean intuitive insight into how our system responds to unknown signals.

We experimented with various RF emitters including several additional car RKEs, wireless ceiling fan controls, Bluetooth® computer mouse, and Bluetooth® search from a mobile cellular phone. Qualitatively, model $\mathcal{M}_{offset}$ dramatically outperformed model $\mathcal{M}_{clean}$ in all

instances. Many transmitter modulations were correctly identified, with the exception being a RKE in which the receiver was not tuned closely enough to the transmitter's center frequency.

An interesting observation occured with the Bluetooth® devices. The Bluetooth® specification calls for a GFSK modulation at the initiation of device communication and for lower versions of the protocol. Our system indeed identified GFSK as the modulation when the search function was started. Various versions of the protocol also use forms of phase-shift keying, specifically $\frac{\pi}{4}$-DQPSK and 8DPSK, which are closely related to the standard DQPSK used in our training set. Even though our system was not explicitly trained to recognize these exact modulations, it did identify the wireless mouse as using DQPSK, which is the most similar to the true modulation type. Thus, we have circumstantial evidence that our method of AMC is robust to minor modulation alterations, and has learned "abstract" features in the data. This is analogous to the ability to recognize a face in a painting vs. a face in a photograph. The concept of a face is abstract, and a system that has learned such abstract features might recognize it across various mediums, even if brush strokes do not fundamentally resemble photographic pixels.

4. CONCLUSION

The experiments described in this report provide evidence that training data used for machine learning techniques should incorporate varying amounts of error that simulates a receiver frequency mismatch. More generally, this technique falls under the category of data augmentation.

An important lesson is that this augmentation must carefully consider the particular aspects of the sensory domain, in this case, radio receivers and I/Q data. This is in contrast to a visual sensor, where augmentations would be related to two-dimensional pixel representations, such as image translation and rotation. Thus, for radio signals, we should look to those augmentations specific to the radio domain. Future work should consider further investigation into these RF-specific signal augmentations for further improvements in machine learning.

REFERENCES

1. O. Vinyals, A. Toshev, S. Bengio, and D. Erhan. 2015. “Show and Tell: A Neural Image Caption Generator,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 3156–3164). June 7–12, Boston, MA.

2. E. J. Humphrey, J. P. Bello, and Y. LeCun. 2012. “Moving Beyond Feature Design: Deep ctures and Automatic Feature Learning in Music Informatics.” *Proceedings of the 13th International Society for Music Information Retrieval (ISMIR) Conference* (pp. 403–408). May 8–12, Porto, Portugal. FEUP edições.

3. O. Dobre, A. Abdi, Y. Bar-Ness, and W. Su. 2007. “Survey of Automatic Modulation Classification Techniques: Classical Approaches and New Trends,” *IET Communications*, vol. 1, no. 2, pp. 137–156.

4. B. Migliori and D. Gebhardt. 2016. “Biologically Inspired Machine Learning for Radio Signal Modulation Classification.” Technical Report 3025. Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA.

5. T. J. O’Shea and J. Corgan. 2016. “Convolutional Radio Modulation Recognition Networks,” Computing Research Repository (CoRR). Abstract available online at http://arxiv.org/abs/1602.04105.

6. J. Gibson. 2002. *The Communications Handbook*, The Electrical Engineering Handbook Series, CRC Press. Boca Raton, FL.

7. GNU Radio website: http://www.gnuradio.org. Accessed July 2015.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
September 2016	Final	

4. TITLE AND SUBTITLE

Radio Signal Augmentation for Improved Training of a Convolutional Neural Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

Daniel Gebhardt, Ph.D.
Benjamin Migliori, Ph.D.
Logan Straatemeier
Michael Walton

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific
53560 Hull Street
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 3055

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SSC Pacific
Naval Innovative Science and Engineering (NISE) Program
53560 Hull Street
San Diego, CA 92152–5001

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Aproved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This technical report presents the findings of an experiment to evaluate the effectiveness of our technique for improving the accuracy of identifying which type of digital modulation is present in a sample of radio signal data. We use a convolutional neural network (CNN) to identify the modulation type from raw digitized radio signal input. The CNN is trained using our technique of dataset augmentation, which applies a transformation specific to the sensory domain of radio (and potentially, closely related signal types). This augmentation simulates a receiver's clock offset or error.

Digital radio signal receivers will have a clock frequency slightly different than the transmitter, even if each is tuned to the "same" frequency. This is usually accounted for in the receiver design, referred to as carrier clock recovery, since it is designed for a known signal type. Our method is to apply varying amounts of clock frequency offset to a training dataset, and use it to train the machine learning algorithm (in this case, a CNN). The trained CNN model is compared to a baseline model in which no clock offset was used during training.

Classification performance increases to nearly 100% when trained with frequency offset, compared to the baseline of 58%. Two real-world signals were captured from car remote keyless entry fobs. These signals contain an unknown receiver clock offset. The network trained with our method classified nearly 100% of the samples correctly, while the baseline network did not correctly identify the on-off keying (OOK) modulation. A recommended action is to further investigate dataset augmentation, especially in the domain of radio signals. This domain could benefit from very specific, but very useful, transforms to further improve performance of machine learning techniques.

15. SUBJECT TERMS

digital modulation; radio signal data; convolutional data network; dataset augmentation; clock offset; machine learning algorithm; frequency offset; on-off keying modulation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Daniel Gebhardt
U	U	U	U	14	**19B. TELEPHONE NUMBER** *(Include area code)* (619) 553-2796

INITIAL DISTRIBUTION

84500	Library	(1)
56120	D. Gebhardt	(1)
56140	L. Straatemeir	(1)
56150	B. Migliori	(1)
56150	M. W. Walton	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001